1. A method performed at a network interface unit (NIU) for communicating data packets over a non-secure network between client devices on a local area network (LAN) and an access node for a secure virtual private network (VPN) comprising

authenticating at least one of said client devices seeking to access said VPN, thereby establishing at least one authenticated client device,

sending configuration information from a configuration server at said NIU to said authenticated client devices,

sending at least one menu from a GUI server at said NIU to authenticated client devices,

receiving at least a first message reflecting at least one selection at at least one of said authenticated client devices from said at least one menu, and

means for accessing said non-secure network using information in said at least a first message, and

establishing a secure connection between said non-secure network and said access node using a security server at said NIU.

2. The method of claim 1 wherein said configuration information for each authenticated client device comprises information received on behalf of each of said client devices upon an initial authenticating of respective ones of said client devices.

3. The method of claim 1 wherein said authenticating comprises

sending a GUI page to each client device seeking access to said VPN, said GUI page soliciting authentication information, and

receiving authentication information from client devices seeking access to said VPN, and

authenticating said at least one client device seeking access to said VPN when received authentication information bears a predetermined relationship to information stored at said NIU for respective ones of said client devices.

4. The method of claim 1 further comprising storing a plurality of web pages for use by said GUI server.

5. The method of claim 1 wherein said at least one menu comprises a main menu comprising selections corresponding to predefined access connections to said non-secure network.

6. The method of claim 5 wherein said first message comprises information indicating a selection of a predefined access connection to said non-secure network.

7. The method of claim 6 wherein said predefined access connection is a dial-up connection and said accessing of said non-secure network is accomplished using configuration information corresponding to said dial-up connection.

8. The method of claim 5 wherein said first message comprises information indicating a selection of a predefined type of access connection to said non-secure network.

9. The method of claim 8 further comprising sending a second menu from said GUI server to a client device seeking access to said VPN in response to said first message, said second menu including information regarding at least one connection to said non-secure network, said second menu including only information for connections of only said predefined type.

10. The method of claim 9 wherein said predefined type of connection is a dial-up connection.

11. The method of claim 9 wherein said predefined type of connection is a network connection employing a fixed IP address.

12. The method of claim 9 wherein said predefined type of connection is a network connection employing a temporary IP address.

13. The method of claim 12 further comprising accessing a DHCP server at said NIU to obtain said temporary IP address.

14. The method of claim 12 further comprising accessing a DHCP server in said non-secure network to obtain said temporary IP address, said accessing of said DHCP server comprising employing a DHCP client at said NIU to access said DHCP server in said non-secure network.

15. The method of claim 9 wherein said predefined type of connection is a network connection employing a fixed point-to-point over Ethernet (PPPoE) address.

16. The method of claim 5 wherein said first message comprises information indicating a request for a new connection to said non-secure network.

17. The method of claim 16 further comprising sending a form from said GUI server to a client device seeking access to said VPN in response to said first message, said form soliciting information regarding said new connection.

18. The method of claim 17 wherein said new connection is a dial-up connection, and said information solicited by said form comprises dial-up information relating to said new connection.

19. The method of claim 18 wherein said new connection is a network connection, and said information solicited by said form comprises network information relating to said new connection.

20. The method of claim 16 further comprising storing information received from a client device responding to said form, said information being stored as configuration information associated with said responding client device relating to a connection of an indicated type.

21. The method of claim 20 wherein said storing configuration information comprises storing configuration information in a removable memory module.

22. A method practiced at a network interface unit (NIU) for communicating data packets over a non-secure network between client devices on at least one local area network (LAN) and at least one access node of a secure virtual private network (VPN), the method comprising

receiving data packets from said devices by way of said LANs,

multiplexing said data packets into at least one packet data stream,

modifying said packet data streams in a security server in accordance with a secure communications protocol by encrypting packets in said data streams and encapsulating resulting encrypted packets,

providing network destination address information from a DNS server for at least selected ones of said data streams.

23. The method of claim 22 wherein said modifying said packet data streams in a security server comprises modifying said packet streams in an IPsec server.

24. The method of claim 23 further comprising

receiving at least one stream of data packets from said non-secure network, filtering out packets in said streams of received packets that are not from said VPN network, said filtering being performed by a firewall in said security server,

modifying said packets in said at least one stream by decrypting said packets in said at least one received data stream and decapsulating resulting decrypted packets, said decrypting and decapsulating being performed by said security server,

demultiplexing said at least one stream of received data packets to form at least one demultiplexed stream of data packets for delivery to said at least one LAN.

25. The method of claim 24 further comprising

authenticating client devices on said at least one LAN, and

wherein packets from authenticated client devices on said at least one LAN that are received at said network interface device are processed as packets received from said VPN.